Exhibit 43

EMERY CELLI BRINCKERHOFF & ABADY LLP

ATTORNEYS AT LAW
600 FIFTH AVENUE AT ROCKEFELLER CENTER
10th FLOOR
NEW YORK, NEW YORK 10020

RICHARD D. EMERY
ANDREW G. CELLI, JR.
MATTHEW D. BRINCKERHOFF
JONATHAN S. ABADY
EARL S. WARD
ILANN M. MAAZEL
HAL R. LIEBERMAN
DANIEL J. KORNSTEIN
O. ANDREW F. WILSON
ELIZABETH S. SAYLOR
DEBRA L. GREENBERGER
ZOE SALZMAN
SAM SHAPIRO
ALISON FRICK
DAVID LEBOWITZ
HAYLEY HOROWITZ
DOUGLAS E. LIEB
ALANNA SMALL
JESSICA CLARKE

TELEPHONE
(212) 763-5000
FACSIMILE
(212) 763-5001
WEB ADDRESS
www.ecbalaw.com

CHARLES J. OGLETREE, JR.
DIANE L. HOUK

December 4, 2016

Via Email

Mark Wolosik
Division Manager
Allegheny County Elections Division
mark.wolosik@alleghenycounty.us

Re: Examination of Voting Machines During December 5 Recount

Dear Mr. Wolosik:

This firm represents presidential candidate Jill Stein and her campaign, in support of the efforts of hundreds of Allegheny County voters who have sought a recount and recanvass in Allegheny County of the 2016 vote for President and Senate. As ordered by the Honorable Joseph M. James on Friday, December 2, that recount and recanvass is scheduled to take place on Monday, December 5 at 10:00 am.

I write to explain why the Election Division, as agent of the Allegheny County Board of Elections, has the authority and in fact the duty to permit forensic examination by independent experts of the election management computers and a sampling of the electronic voting machines and removable media used in the 2016 general election. This letter will serve as a formal request, on behalf of Dr. Stein and her campaign, to allow such a forensic examination at the campaign's expense and under the supervision of the Elections Division.

Candidates Are Statutorily "Entitled" to "Examine" the DRE Voting System

The rights of candidates during recounts are broad: "Any candidate, attorney or watcher present at any recount of ballots or recanvass of voting machines *shall be entitled to examine . . . the voting machine and to raise any objections regarding the same*, which shall be decided by the county board, subject to appeal, in the manner provided by this act." 25 P.S. § 2650(c) (italics added.) The statute does not define "examine," but plainly an examination is considerably more searching than simply watching a recanvass. To examine means "to inspect closely," to "test the condition of," to "inquire into carefully." *See Examine*, Merriam-Webster Dictionary, http://www.merriam-webster.com/dictionary/examine.

Allegheny County, of course, uses a DRE electronic voting system, and in particular the iVotronics system. Dr. Stein is entitled under the statute to "test the condition" of that system, and to "inspect" it "closely." That necessarily *requires* a forensic examination of the DRE software, removable media, and electronic management system. The only way to "test the condition" of the DRE system is to examine the software. As explained in the affidavit of J. Alex Halderman attached to the petitions for a recount or recanvass, "Paperless DRE voting machines do not create any physical record of each vote, so forensic examination of the equipment is the only way to assures that the machines were not manipulated in a cyberattack." Halderman Aff. ¶ 15.

At the hearing on Friday, you testified about the importance of ensuring that the firmware associated with the system is in good working order and is in fact the same version of the firmware certified for use in the machines. That is why Allegheny County admirably chooses to conduct pre-election checks of the firmware on a random sample of its DRE machines sixty days before every election. You also testified that this process is neither logistically nor financially burdensome. Forensic experts agree. *See* Buell Aff. ¶¶ 32-38. We are asking for an essentially similar process to the one you conduct before the election to occur on a larger sample of machines, at the expense of Dr. Stein's campaign, and *after* the election to ensure the integrity of the vote with certainty.

The statute is plain, as is the duty of the Board. Dr. Stein, by her representatives, is entitled to examine the DRE voting system used in Allegheny County in connection with the recanvass Allegheny County will conduct. We have top computer experts ready to do so, on one day's notice, under the careful supervision of the Elections Division. Dr. Stein's campaign will even pay for these experts. Between a voter and the election result is the DRE system. The system must be examined.

The Supreme Court of Pennsylvania Gives the Board Broad Power to Permit Forensic Examination of the DRE System

"Nothing can be more vital towards the accomplishment of an honest and just selection than the ascertainment of the intention of the voter." *Appeal of McCracken*, 370 Pa. 562, 566 (1952). Mere recanvassing of the DRE voting machines is insufficient to fulfill the Board's "apparent and impelling" duty to ascertain[] *for whom* votes were cast." *McCracken*, 370 Pa. at 566 (emphasis in original). As the Pennsylvania Supreme Court has held, "[i]n the computation of the vote, [the Board's] functions are not limited to those of a humanized adding machine. The Board is not a multiple comptometer." *Id.* at 565. Rather, "canvassing and computing necessarily embrace acts of discretion." *Id.*; *see In re Recount of Ballots of Rome Twp., Crawford Cty.*, 397 Pa. 331, 332 (1959) (the Pennsylvania Election Code is "a *highly remedial statute* which should be *liberally construed* in order to secure a proper computation of the votes cast at an election.").

"There could scarcely be a duty more apparent and impelling on an Election

Board than that of ascertaining *for whom* votes were cast." *McCracken*, 370 Pa. at 565. In counties with optical scan ballots, the Board can fulfill that "impelling" duty by manually counting the papers ballots. Allegheny County, though, has no paper ballots. Without paper verification, the *only* way for the Board to fulfill that duty is to permit a complete, sophisticated forensic analysis by computer experts of DRE machines, removable media, and the election management computers used to program the machines and tally results.

"The needs of our democracy require accurate and rapid ascertainment of the people's will. And it is for that reason that the Legislature has entrusted the County Board of Elections with plenary powers in the administration of the election code." *Id*. In this case, in this election, and with these machines, the only way to ensure the integrity of the vote in this county is a comprehensive forensic exam.

Conclusion: The Board Should and Must Permit A Forensic Examination of the DRE System

We therefore request that, in connection with the recanvass and recount scheduled to proceed on December 5, 2016, the Commission permit forensic examination of the DRE electronic voting system. In support of this request, attached please find the affidavits of leading computer experts Duncan Buell, J. Alex Halderman, Harri Hursti, Daniel Lopresti, Candice Hoke, and Matthew Bishop, all of which speak to the vulnerabilities of electronic voting systems, including the DRE system used in Allegheny County in the 2016 election, and the desirability and feasibility of a forensic audit.

Thank you for your consideration.

Respectfully,

/s/

Douglas E. Lieb*

* *Admitted pro hac vice*

Encl.

c. Al Opsitnick, Esq.
Ronald L. Hicks and Nicholas L. Bell, Esqs.
Stuart C. Gaul, Jr., Esq.

AFFIDAVIT OF DUNCAN A. BUELL

DUNCAN A. BUELL, being duly sworn, deposes and says the following under penalty of perjury.

1. I am a professor of Computer Science and Engineering at the University of South Carolina. I submit this affidavit in support of petitions to recount/recanvass the vote in Allegheny County.

2. In my opinion, the electronic voting system used by Allegheny County, called the iVotronics system, is vulnerable to malicious interference and inadvertent error. The system is unreliable. The only way to be sure of an accurate tally of the vote in this election is to conduct a forensic analysis of the machines and software. Such an evaluation could be accomplished expeditiously, in a few short hours, and would allow us to know whether the vote tally in Allegheny County was accurate.

Qualifications and Relevant Employment History

3. In 1971, I earned a B.S. in Mathematics from the University of Arizona. The following year, I earned an M.A. in Mathematics from the University of Michigan. In 1976, I earned a doctorate in Mathematics, with an emphasis in number theory, from the University of Illinois at Chicago. A copy of my resume is available on my university website at http://www.cse.sc.edu/duncanbuell.

4. Since 2000, I have been a Professor in the Department of Computer Science and Engineering at the University of South Carolina. From 2000 to 2009, I served as Chair of that department. During 2005-2006, I served as Interim Dean of the College of Engineering and Information Technology at the University of South Carolina.

In my management capacity as department chair, my duties also included the management of the college's information technology staff and its network and computer center, which included 9 instructional labs with approximately 250 desktop computers. I was also responsible for the management and operation of cluster computers, file and mail servers, and the college's network infrastructure.

5. Prior to 2000, I was for just under 15 years employed (with various job titles and duties) at the Supercomputing Research Center (later named the Center for Computing Sciences) of the Institute for Defense Analyses, a Federally Funded Research and Development Center (FFRDC) supporting the National Security Agency. Our mission at SRC/CCS was primarily to conduct research on high performance computing systems and computational mathematics to ensure that those computing systems would be suitable for use by NSA, since the NSA workload has technical characteristics different from most high-end computations like weather modeling. While at IDA I played a leading role in a group that received a Meritorious Unit Citation from Director of Central Intelligence George Tenet for what was then "the largest single computation ever made" in the U.S. intelligence community.

6. In 2013, I was elected a Fellow of the American Association for the Advancement of Science. In 2016, I was appointed to the NCR Chair in Computer Science and Engineering at the University of South Carolina.

7. My current research interests include electronic voting systems, digital humanities, high performance computing applications, parallel algorithms and architecture, computer security, computational number theory, and information retrieval.

Over the past 40 years, I have published articles in peer-reviewed journals and/or lectured on each of these topics.

8. Since about 2004 I have been working with the League of Women Voters of South Carolina (LWVSC) as an unpaid consultant on the issue of electronic voting machines. South Carolina uses statewide the ES&S iVotronic terminals and the corresponding Unity[1] software. Beginning in summer 2010, I worked with citizen volunteer activists Frank Heindel, Chip Moore, Eleanor Hare, and Barbara Zia on acquisition by FOIA of the election data from the November 2010 general elections in South Carolina and on the analysis of that data. That work, based on data we acquired by FOIA, culminated in an academic paper that was presented at the annual USENIX EVT/WOTE (Electronic Voting Technology Workshop/Workshop on Trustworthy Elections) conference in August 2011. My work with the LWVSC has continued, in that when the state of South Carolina acquired the 2010 election data from the counties and posted it on the SCSEC website, I analyzed that data as well.

Basis for My Opinions

9. I base the opinions in this affidavit on my knowledge, skill, training, education, and experience: I have been programming computers for more than 45 years and have been employed as a computer scientist for more than 35 years, working with

[1] Unity is the election management software suite, a number of programs that run on a Microsoft computer at county headquarters and perform such tasks as initializing the database with jurisdiction and candidate information, configuring the ballot styles, collecting the vote totals from the PEBs into the master database of votes and log information, and producing reports of votes by candidate and precinct as well as the log files and cast vote record files referred to below.

computers and computer applications and operations and management of large computer networks, including file and mail servers that utilize the Internet.

10. I have also used for my opinions the analysis of the ES&S iVotronic system and the Unity software done for Ohio Secretary of State Jennifer Brunner and published 7 December 2007. This is the "EVEREST Report" and is still the best and most complete analysis of the iVotronics and their accompanying software and procedures. I am also familiar with the report produced for the state of Florida ("the Yasinsac report") after the 2006 election in Sarasota, Florida resulted in a very high undervote in the race for U. S. Representative.

11. I also base my opinions on my analysis of ES&S election data using computer programs I have written. I first wrote these programs to analyze the 2010 General Election data from South Carolina. I have subsequently analyzed the 2012, 2014, and 2016 data from South Carolina. I have also used my programs to analyze data from from Hidalgo County, Texas and from Venango County, Pennsylvania, at the request of election officials there. I believe I have more experience in doing this analysis of ES&S iVotronic data than anyone else, possibly including employees of ES&S itself.

The ES&S iVotronics Machines and Accompanying System Are Riddled with Software and Procedural Vulnerabilities

12. The iVotronics machines and software systems[2] are not secure or reliable. They are susceptible to both intentional and malicious interference as well as errors

[2] I will refer throughout this affidavit to "the iVotronics" and mean by that the entire system of which the iVotronic is the voting machine itself. The system includes also the handheld PEB devices, the flash memory cards inserted into and removed from the iVotronic, and the Unity software and stored data used (usually) at county headquarters.

resulting from inadvertent or sloppy mistakes. The only way to be sure of the accuracy of the vote is to carefully examine the machines and the systems they ran.

The Machines Are Vulnerable to Intentional Interference

13. The EVEREST report documented a number of software flaws, many of which relate to the reliability or security of the system. The Yasinsac report describes a naïve, indeed juvenile, password structure that could easily be circumvented by any insider and that could be circumvented without enormous difficulty by an outside attacker.

14. The EVEREST report also refers to numerous buffer overflow vulnerabilities that would permit the installation of malicious software. And, when done by a skilled attacker, the malicious code could eventually erase itself to leave no trace.

15. In addition, an attacker could use a PEB[3] or a PEB emulator (a Palm Pilot with the same infrared protocol was used in the test) to masquerade as a valid PEB, open an iVotronic as if for voting, and upload malicious code.

16. Election officials and vendors often justify the security of their systems by pointing to the proprietary nature of the hardware and software, suggesting that no one who was not permitted to use a voting system could get access to one. This argument is incorrect; I purchased two iVotronics with PEBs myself on eBay. It would be relatively straightforward to create a rogue PEB through which to spread malware (thus not needing

[3] Personal Electronic Ballot: This is a handheld device slightly smaller than a paperback novel. Proper procedure is that the precinct poll manager will use one particular PEB to open and close the iVotronics at the beginning and ending of Election Day, and that regular poll workers will use a different set of PEBs to open the iVotronic for each voter and to load onto the machine the particular ballot style for that voter's jurisdictions.

the Palm Pilot or similar device). In my experience as a poll observer in South Carolina in the 2016 General Election, I noticed that it would have been easy for a voter to shield from view the PEB slot while voting and thus insert a rogue PEB to upload malicious code.

The Machines Are Vulnerable Even If They Are Not Connected to the Internet

17. It is a frequent claim by election officials that the voting machines cannot be corrupted because they are never "connected" to the Internet. This is a statement that is only true if literally none of the computing hardware—or any removable media connected to the computer—has ever been connected to any computer that has been connected to the Internet.

18. To provide background for what is really meant by "not connected," one must remember what apparently took place with the Stuxnet virus. Stuxnet was apparently a joint US and Israeli effort to sabotage the Iranian efforts to produce nuclear weapons. Part of the Iranian nuclear program involved specific centrifuges for concentrating uranium. None of those centrifuges were ever "connected" to the Internet, and yet Stuxnet was inserted into the Iranian nuclear network and caused a large number of centrifuges to self-destruct. Part of the distribution of the Stuxnet virus apparently involved hiding it on flash memory drives that were sprinkled in parking lots. When curious people picked them up and inserted them into computers inside the nuclear program network, Stuxnet was inserted into the system.

19. Indeed, this vulnerability is well known. My colleagues and I received a briefing from the FBI a few years ago warning faculty travelling to conferences not to

allow a "friend" to offer us a flash drive to share documents, because the "friend" could easily install a virus in this way.

20. In short, any sort of electronic connection can lead to the insertion of malware into the computer thus connected.

21. In most electronic voting systems in the United States, including the iVotronics, a county election official uses the computer running Unity to prepare the ballot styles for each of the precincts and jurisdictions. The county computer then prepares the PEBs for use on Election Day by loading the PEBs with the ballot styles for the individual precincts. The county computer would normally also erase the files on the memory cards to be inserted into the iVotronics. That represents the outward path from county headquarters to the individual iVotronics.

22. On the inbound path, at the end of Election Day, the memory cards and the PEBs come back from the individual precincts and are connected to the county computer. Presumably this is the same computer from which results are provided to the media and the public at the end of Election Day.

23. It can only be argued that this voting system as a system is "not connected" to the Internet if it is the case that none of the computing equipment has been connected at any time. This means that the Unity computer will never have had its operating system or its code updated since the system was first brought up (unless, of course, the updates were to come on some medium like a CD from a trusted source like the ES&S vendor). This means that flash drives that carry results from the Unity system to a computer on the network that sends the results to the news media (or any flash drive that has ever been

inserted into a computer on a network) must never be reused and inserted back into the Unity system.

24. It is possible that all these security measures are in place in every single county in the state. In my experience, however, this is extremely unlikely, and thus a forensic analysis would need to look at and verify that all these protocols were followed.

The Machines Are Also Vulnerable to Inadvertent Errors that Render Them Unreliable

25. The complexity of the iVotronics system itself leaves it vulnerable to error. For example, the iVotronics are supposed to be opened and closed with a single PEB in each precinct, with that PEB used only for opening and closing. Since at closing the vote totals are collected into the PEB, and the totals from the closing PEB are used for totaling into the Unity database at county headquarters, it can (and does) happen that poll managers don't follow directions and use multiple PEBs for opening and closing, and that not all the vote totals are accumulated into the county database. PEBs can also fail in a precinct.

26. I have also seen examples when iVotronics would not open normally at the beginning of Election Day, were opened later by a technician, but then at the end of Election Day the paper tape produced by the precinct poll manager said "Machine not opened". This has led to the votes in those machines not being accumulated into the official count at the county level and thus effectively not being counted.

27. Another failure in the software comes when the ballot definition in the iVotronic is different from that at county headquarters. If the county system lists two

races for county council, say, and the ballot definition in the iVotronic only has one race, then what happens is essentially that vote totals from that point on down to the bottom of the ballot are shifted up one row and added into the wrong row's totals.

28. Similar failures can occur when memory cards fail, or when iVotronics will not allow themselves to be closed for some reason.

Only a Forensic Evaluation Can Determine Whether Votes Were Properly Counted

29. Only a forensic evaluation, including an examination of the election management system and software, will reveal whether the official tally of votes is reliable or whether the voting process was disrupted by malicious attack or other error.

30. With respect to malicious interference, a forensic evaluation would allow investigators certainly to determine if a systematic failure of proper procedures had occurred. I would expect random failures to occur, reflecting the chaos of Election Day and the imperfections of poll workers. Systematic issues, however, would show up as anomalies that might well be intentional. The ability to drill down to precinct level data allows one to compare anomalies and "errors" against voting preferences and demographics, and a forensic analysis with statistics would spot such anomalies.

31. Such an investigation could be accomplished expeditiously. For the purpose of my data analysis, I would need the EL152 event log file, the EL155 cast vote record, the EL68A system file, and the EL30A results file. I have never been told in South Carolina, Hidalgo County (TX), or Venango County (PA)—each places I have worked and performed analyses of election data—that obtaining this data was difficult; it can be produced using the Unity software from the county database. Analysis of this data using

my programs for the entire 2016 South Carolina data (2.1 million total votes) took about *three hours*' compute time. Depending on the number of exceptional cases to be looked into, an in-depth examination of these cases should take only a small number of days, much less time if the exceptions are usually benign. (For example, I produce a list of iVotronics that appear in the event log but have no cast vote record. It has happened that such a machine has not had its votes counted, which is a serious error, but what I usually see here is that such a machine never did get properly opened and was never used; that fact can be determined by a very quick scan of the event log that takes only seconds.)

32. I have conducted forensic analyses of these machines to ensure that the voting tallies were accurate. Beginning with the 2010 General Election in South Carolina, I obtained the voting data and wrote my own programs to verify that all the votes had in fact been counted and that the election data was at least internally consistent. I have rewritten my programs several times, most recently following the 2016 General Election. I have used four data sources in my analysis, which are data files published as public records by the South Carolina State Election Commission on their website http://scvotes.org.

33. First, I examine the event log file from each iVotronic. It lists the events recorded in each machine since the most recent time the internal file was erased. From this file I get the serial number of the iVotronic machine, the serial numbers of the PEBs used for most of the events, the timestamp when the events occurred, and the code number and expanded English text of the event itself. For example, code 1510 is "Vote cast by voter." From this file I can determine that the internal memory was zeroed before

use for this election, how many votes were cast on each iVotronic, which PEB was used for opening and for closing, verify that the iVotronic was closed and its internal data written to the memory card, and so forth. This allows me to determine the number of votes cast on each machine, the fact that the machines were cleared of votes and that the data was written to the memory cards, and whether or not the machine was functioning properly on Election Day. By knowing which PEB was used for closing I also know which PEB serial numbers to look for in the system log to verify that the vote totals were correctly uploaded to the county database. I have repeatedly observed instances of "cranky" iVotronics that could not be closed or that had bad memory cards, or were not functioning properly; knowing that such machines exist (by serial number) allows me to verify elsewhere that other methods have been used to account properly for the votes in those iVotronics.

34. Second, I examine the system log for the Unity software running on a Microsoft computer at county headquarters. From this file I can determine that the county database was cleared before Election Day, that the correct number of votes were uploaded from the PEBs (by serial number) for a given precinct, that the memory card data was uploaded to the county database, and so forth. It is in this file that one can find the log of ballot definition differences between the county version and the version in each iVotronic. This allows me to determine that the data (including vote counts) from machines known to have been used for voting has been uploaded correctly.

35. Next, I look at the data of the actual cast vote record, in a randomized order, and with no identifying information about which voter cast which ballot. From this

file I can produce vote counts for each iVotronic, each ballot style, each precinct, and each race.

36. Finally, I examine one of several "results" files that are produced by the Unity software. From this I can determine for each precinct and each race the number of iVotronic votes recorded from the PEBs, the number of votes that might have been recorded by reading directly from the memory cards, and the number of paper or absentee ballots. (If the county chooses not to print this information, it might not appear.)

37. My programs count votes at the precinct/iVotronic/ballot style/race level, votes from the "vote cast" codes, and votes from the results file. Discrepancies between these files usually indicate that procedures have not been followed. I verify that iVotronics used for voting have been closed and that the PEB used for closing shows up in the system log file as having the correct number of votes uploaded. I verify that all the memory cards have been collected and their data uploaded, and I identify instances in which the ballot definitions in Unity differed from those in the iVotronics. I also record lists of the events in the event log that indicate that the machines have been malfunctioning and thus might not be recording votes correctly or might not have recorded the correct data, although I am not able to determine what the incorrect entries might be.

38. I have over the course of four General Elections now seen instances of probably all the different errors that could occur. Assuming there is a record in these files of any of the hardware by serial number, then my programs will detect an inconsistency and report that in an EXCEPTIONS file.

Conclusion: A Forensic Audit Is the Only Way to Have Confidence in the Vote Tally

29. For the reasons stated above, the electronic voting systems in place in Pennsylvania (including Allegheny County) are unreliable and vulnerable to attack. That is why other jurisdictions have discontinued the use of some electronic voting machines.

30. There were well-publicized attacks on America's voting infrastructure this year by foreign agents and other hostile forces, attacks confirmed by the United States' government's security agencies.

31. Given this reality, and given the vulnerability of the electronic machines used here, it is crucial that computer experts be able to forensically evaluate the electronic voting data from Allegheny county to ensure that the vote was counted accurately.

32. I affirm that the foregoing is true and correct.

Duncan Buell 2 Dec 2016
DUNCAN BUELL Date

Sworn before me this 2nd day of December, 2016, in Columbia, SC.

Rebecca Mayo
NOTARY PUBLIC

AFFIDAVIT OF J. ALEX HALDERMAN

J. ALEX HALDERMAN, being duly sworn, deposes and says the following under penalty of perjury:

1. My name is J. Alex Halderman. I am a Professor of Computer Science and Engineering and the Director of the Center for Computer Security and Society at the University of Michigan in Ann Arbor, Michigan. I submit this Affidavit in support of the petitioners.

2. I have a Ph.D., a Master's Degree, and a Bachelor's Degree in Computer Science, all from Princeton University.

3. My research focuses on computer security and privacy, with an emphasis on problems that broadly impact society and public policy. Among my areas of research are software security, data privacy, and electronic voting.

4. I have authored more than seventy articles and books. My work has been cited in more than 4,700 scholarly publications. I have served on the program committees for thirty research conferences and workshops, and I co-chaired the USENIX Election Technology Workshop, which focuses on electronic voting security. I received the John Gideon Award for Election Integrity from the Election Verification Network, the Alfred P. Sloan Foundation Research Fellowship, the IRTF Applied Networking Research Prize, and the University of Michigan College of Engineering 1938 E Award for teaching and scholarship.

5. I have published peer-reviewed research analyzing the security of electronic voting systems used in Pennsylvania, other U.S. states, and other countries. I was part of a team of experts commissioned by the California Secretary of State to conduct a "Top-to-Bottom" review of the state's electronic voting systems. I have also investigated methods for improving the

security of electronic voting, such as efficient techniques for testing whether electronic vote totals match paper vote records.

6. My full curriculum vitae, including a list of honors and awards, research projects, and publications, is attached as Exhibit A.

Context: Cyberattacks and the 2016 Presidential Election

7. The 2016 presidential election was subject to unprecedented cyberattacks apparently intended to interfere with the election. This summer, attackers broke into the email system of the Democratic National Committee and, separately, into the email account of John Podesta, the chairman of Secretary Clinton's campaign. Exhibits B and C. The attackers leaked private messages from both hacks. Attackers also infiltrated the voter registration systems of two states, Illinois and Arizona, and stole voter data. Exhibit D. The Department of Homeland Security has stated that senior officials in the Russian government commissioned these attacks. Exhibit E. Attackers attempted to breach election offices in more than 20 other states. Exhibit F.

8. Russia has sophisticated cyber-offensive capabilities, and it has shown a willingness to use them to hack elections elsewhere. For instance, according to published reports, during the 2014 presidential election in Ukraine, attackers linked to Russia sabotaged Ukraine's vote-counting infrastructure, and Ukrainian officials succeeded only at the last minute in defusing vote-stealing malware that could have caused the wrong winner to be announced. Exhibit G. Countries other than Russia also have similarly sophisticated cyberwarfare capabilities.

9. If a foreign government were to attempt to hack American voting machines to influence the outcome of a presidential election, one might expect the attackers to proceed as follows. First, the attackers might probe election offices (or the offices of election service vendors) well in advance to find ways to break into the computers. Next, closer to the election,

when it was clear from polling data which states would have close electoral margins, the attackers might spread malware into voting machines in some of these states, manipulating the machines to shift a few percent of the vote to favor their desired candidate. One would expect a skilled attacker's work to leave no visible signs, other than a surprising electoral outcome in which results in several close states differed from pre-election polling.

The Vulnerability of American Voting Machines to Cyberattack

10. As I and other experts have repeatedly documented in peer-reviewed and state-sponsored research studies, American voting machines have serious cybersecurity problems. Voting machines are computers with reprogrammable software. An attacker who can modify that software by infecting the machines with malware can cause the machines to provide any result of the attacker's choosing. As I have demonstrated in laboratory tests, in just a few seconds, anyone can install vote-stealing malware on a voting machine that silently alters the electronic records of every vote.[1]

11. Whether voting machines are connected to the Internet is irrelevant. Sophisticated attackers such as nation-states have a developed a variety of techniques for attacking non-Internet-connected systems.[2] Shortly before each election, poll workers copy the ballot design from a regular desktop computer in a government office (or at a company that services the voting machines) and use removable media (akin to the memory card in a digital camera) to load the ballot design onto each machine. That initial computer is almost certainly not well enough secured to guard against attacks by foreign governments. If technically sophisticated attackers infect that computer, they can spread vote-stealing malware to every voting machine in the area.

[1] A video documenting this result is publicly available at https://youtu.be/aZws98jw67g.

[2] A well known example of this ability, which is known as "jumping an airgap", is the Stuxnet computer virus, which was created to sabotage Iran's nuclear centrifuge program by attacking factory equipment that was not directly connected to the Internet: https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/.

Most voting machines also have reprogrammable software ("firmware") that can in many cases be manipulated well in advance of the election to introduce vote-stealing malware. Technically sophisticated attackers can accomplish this with ease.

12. While the vulnerabilities of American voting machines have been known for some time, states' responses to these vulnerabilities have been patchy and inconsistent at best. Many states, including Pennsylvania, continue to use out-of-date machines that are known to be insecure.

13. Procedural safeguards used by Pennsylvania and other states to protect their voting equipment are inadequate to guard against manipulation of the election outcome via cyberattack. These inadequate safeguards include tamper evident seals, protective counters, and test decks.

14. Tamper evident seals do not protect against remote electronic attackers, and may not even defend against local attackers. The types of seals typically used for voting equipment can be bypassed without detection using readily available tools.[3] For some seals, these include screwdrivers and hair dryers. By bypassing the seals, an attacker with physical access to the voting machines can modify their internal programming to make them output fraudulent results.

15. Malware installed on a voting machine can subvert the protective counter by changing its value in the machine's computer memory. Malware can subvert test decks by refraining from cheating when only a small number of ballots have been scanned (as is the case when a test deck is used), or by only cheating at a specified time of day (electronic voting machines typically have internal clocks).

[3] https://www.cs.princeton.edu/~appel/voting/SealsOnVotingMachines.pdf

Pennsylvania's Voting Machines Are Among The Most Vulnerable In The U.S.

16. Paper ballots are the best and most secure technology available for casting votes. Optical scan voting allows the voter to fill out a paper ballot that is scanned and counted by a computer. Electronic voting machines with voter-verified paper audit trails allow the voter to review a printed record of the vote he has just cast on a computer. Only a paper record documents the vote in a manner that cannot later be modified by malware or other forms of cyberattacks.

17. More than 70% of American voters have their votes recorded on some form of paper, which provides permanent evidence of their intent in the event of a post-election recount. In Pennsylvania, less than approximately 20% of votes are cast using paper ballots or voter-verified paper audit trails. The remaining approximately 80% are cast on paperless direct-recording electronic (DRE) computer voting machines that do not create a paper record of each vote.

18. Paperless DRE voting machines have been repeatedly shown to be vulnerable to cyberattacks that can change or erase votes, cast extra votes, or even infect the software used to tabulate results. Since paperless DREs do not generate a physical record of the vote, these attacks may be difficult or impossible to detect or to reverse. There is a broad scientific consensus that paperless DREs do not provide adequate security against cyberattacks.

19. To my knowledge, there are six models of DREs presently in use in Pennsylvania. Every one of these models has been examined by security researchers (in some cases, repeatedly), and all have critical security vulnerabilities that could be exploited by attackers to alter the outcome of elections. These vulnerabilities include architectural weaknesses that cannot be repaired through software updates. As a result, every DRE in use in Pennsylvania is vulnerable to cyberattacks.

20. The vulnerable DREs used in Pennsylvania include:

21. **Hart InterCivic eSlate** — This model of machine was examined by security experts as part of the California "Top to Bottom" election technology review[4] and the Ohio EVEREST election system security review[5]. Both studies found significant vulnerabilities, and California subsequently decertified the machine.[6] The memory cards used by eSlates to transfer votes to a central counting computer are vulnerable to undetectable tampering. The internal security mechanisms of the machines are easily defeated, enabling malicious software to change or erase votes, cast extra votes, or modify the eSlate's software or the software of the JBC, the machine used to tabulate votes. These vulnerabilities could allow attackers to compromise large numbers of machines and alter the election outcome.

22. **Sequoia (Dominion) AVC Advantage** — This model of machine has been studied by multiple groups of security researchers. I have extensively analyzed the AVC Advantage, and I published a peer-reviewed security study of the machines in 2009. My study demonstrates that malware can infect the machines and alter votes. Such malware can spread to the machines via the removable memory cartridges that are used to program the ballot design and offload votes.[7] My research additionally shows that such malware can defeat all of the hardware and software security features that are used by the machines. A separate group of researchers performed a security review that also concluded the AVC Advantage has significant vulnerabilities, including that it would be

[4] http://votingsystems.cdn.sos.ca.gov/oversight/ttbr/hart-amended-recert-final-120707.pdf
[5] http://www.patrickmcdaniel.org/pubs/everest.pdf
[6] http://votingsystems.cdn.sos.ca.gov/oversight/ttbr/hart-amended-recert-final-120707.pdf
[7] https://jhalderm.com/pub/papers/avc-evt09.pdf

straightforward to install vote-stealing malware by replacing one firmware chip.[8] Deficiencies of this voting machine are not limited to security vulnerabilities: in the 2008 New Jersey Republican primary, 37 of these machines exhibited a software bug in which the number of votes recorded was higher than the number of voters.[9]

23. **Danaher Shouptronic 1242** — This model of machine was introduced in 1984 and has not had its security features updated in more than 30 years. Cyberattacks have become significantly more sophisticated during that time, and the security features in the machine are unlikely to be able to defend against today's attackers. Researchers at Lehigh University have analyzed the Shouptronic's computer architecture and shown that it is constructed in a very similar manner to the AVC Advantage.[10] This computer architecture subjects the machines to many of the same attacks. Attackers can replace the machines' ROM chips to cause the machines to output fraudulent results. The machines' design makes it extremely likely that malware can infect the machines via the removable memory cartridges that are used to program the ballot design and retrieve vote totals. The Shouptronic has also already been problematic in past elections,[11] malfunctioning and causing significant delays in voting multiple times in Pennsylvania, Tennessee, and Ohio.

24. **Premier/Diebold (Dominion) AccuVote TSX** — I performed a security analysis of the AccuVote TSX as part of the California Top-to-Bottom review[12], and the machine was also studied as part of Ohio's Project EVEREST[13] and by independent security

[8] https://mbernhard.com/advantage-insecurities-redacted.pdf
[9] https://www.usenix.org/legacy/event/evtwote09/tech/full_papers/appel.pdf
[10] https://verifiedvoting.org/downloads/2008Danaher1242-full.pdf
[11] https://w2.eff.org/Activism/E-voting/infosheets2006/ELECTronic1242.pdf
[12] http://votingsystems.cdn.sos.ca.gov/oversight/ttbr/diebold-102507.pdf
[13] http://www.patrickmcdaniel.org/pubs/everest.pdf

researchers[14]. All of these studies found extremely serious security problems. This machine, along with its predecessor the AccuVote-TS, which I studied extensively in a 2007 security review[15], can be exploited by attackers to alter election results. The security features built into the machines are inadequate to defend against cyberattacks, and vote-stealing malware can spread on the machines' removable memory cards. If attackers infect counties' election management system computers, the attacker can spread vote-stealing malware to every voting machine in the county. Moreover, these machines rely on Windows CE as their operating system, software that has not been supported by Microsoft in several years,[16] and has been shown to have significant vulnerabilities itself, beyond those of the election-specific software.[17] A local attacker with physical access to the machines can additionally tamper with them by manipulating the machines' removable memory cards. Access to these cards is protected using a low security lock that can be picked using only a BIC pen.[18] California decertified the Accuvote TSX in 2007.[19]

25. **Sequoia (Dominion) AVC Edge** — Also decertified by California in 2007,[20] this machine has vulnerabilities similar to those of the TSX and the eSlate. In the California Top-to-Bottom review, security experts found that remote attacks could spread malware to the machines and change, steal, or add votes. Furthermore, such malware can persist even if election workers reinstall an uncorrupted version of the election software. The

[14] http://www.blackboxvoting.org/BBVtsxstudy.pdf

[15] http://citpsite.s3-website-us-east-1.amazonaws.com/oldsite-htdocs/pub/ts06EVT.pdf

[16] https://support.microsoft.com/en-us/lifecycle/search?alpha=Microsoft%20Windows%20CE%20.NET%204.0

[17] https://www.cvedetails.com/product/1079/Microsoft-Windows-Ce.html?vendor_id=26

[18] Shown in this video demonstration: https://www.youtube.com/watch?v=vqNJL0fYwSk

[19] http://votingsystems.cdn.sos.ca.gov/oversight/ttbr/diebold-102507.pdf

[20] http://votingsystems.cdn.sos.ca.gov/oversight/ttbr/sequoia-100109.pdf

California study further discovered that malicious software on the machines could conceal vote-tampering from pre-election testing, hiding manipulation of votes and making the machine output appear otherwise normal. The election software running inside the AVC Edge can also be tampered with by a local attacker with physical access to the machine by replacing a memory card inside the machine's case. I demonstrated this vulnerability by hacking one AVC Edge to make it run the arcade game Pac-Man.[21] A real attacker could just as easily modify the software to make the machine cheat in elections.

26. **Election Systems & Software iVotronic** — The iVotronic was studied by security experts as part of Project EVEREST.[22] The investigation found that firmware on these machines contained buffer overflow vulnerabilities, which could be exploited to infect the machines with malware and alter the election outcome. Further vulnerabilities in the machines include that the Personalized Electronic Ballot module (PEB), which is used to program the ballot design before the election, had only trivially circumventable security protections. The EVEREST researchers also found that the cryptographic keys used by the machines to encrypt votes could be easily extracted by attackers, who could then read or manipulate the vote data.

Examining the Physical Evidence is the Only Way to Ensure the Integrity of the Election

27. One explanation for the results of the 2016 presidential election is that cyberattacks influenced the result. This explanation is plausible, in light of other known cyberattacks intended to affect the outcome of the election; the profound vulnerability of American voting

[21] https://jhalderm.com/pacman/

[22] http://www.patrickmcdaniel.org/pubs/everest.pdf

machines to cyberattack; and the fact that a skilled attacker would leave no outwardly visible evidence of an attack other than an unexpected result.

28. The only way to determine whether a cyberattack affected the outcome of the 2016 presidential election is to examine the available physical evidence—that is, the paper ballots (where available), paper audit trail records (where available), and the voting equipment itself.

For DREs With Paper Trails, The Paper Trail Must Be Recounted By Hand

29. For DRE voting machines that generate paper vote records (VVPAT records), the paper must be examined in order to detect potential cyberattacks. Simply commanding the machines to output the vote totals again would not reliably uncover an attack. This is because any attack on the machines during the election would likely have changed the digital record of the votes stored in the voting machines' memory (as well as in any external memory cartridges or cards). Therefore, the digital records do not reliably preserve voters' intent. In contrast, a manual examination of the VVPAT record would expose this style of cyberattack.

For DREs Without Paper Trails, A Forensic Examination Must Be Conducted

30. Most of Pennsylvania's votes are recorded on DRE voting machines that do not generate any paper record of the individual votes. The only way to reliably determine whether the election outcome on these machines was changed by a cyberattack is to forensically examine the election equipment. A complete forensic examination would include examining the machines' hardware and software, their removable media, and the election management system computers used to program the machines and aggregate election results.

31. Forensic examination could reveal evidence of an attack, such as successful attempts to spread malware to the machines. Such evidence could include malware itself, signs of remote intrusion in the election management system, or indicators that digital vote records or other files

were manipulated or deleted. If a forensic examination can determine the manner in which the machines were compromised, it might also allow manipulation of the election result to be corrected.

For Optical Scan Paper Ballots, The Ballots Must Be Recounted By Hand

32. For ballots cast through optical scanners, a manual recount of the paper ballots, without relying on the electronic equipment, is necessary to reliably detect possible hacking. Using optical scan machines to conduct the recount, even after first evaluating the machines through a test deck, is insufficient to detect potential cyberattacks. Attackers intending to commit a successful cyberattack could, and likely would, create a method to undermine any pre-tests.[23]

33. If the optical scanners were attacked by infecting them with malware, such malware might still be active in the scanners during the recount. Recounting the ballots using an infected scanner would likely yield the same results as the original count, despite the results being wrong. If attackers managed to compromise the count during election day but in a manner that did not persist on the machines, machine recounts would still be insufficient. Attackers who were able to infect the machines before the election likely would be able to attack them again, perhaps using the same methods, prior to the recount. The dates and the procedures of the recount are widely publicized, so attackers would know when to strike. This would result in the scanners producing the same incorrect results when the ballots were scanned again.

34. In contrast to machine recounts, a manual recount, where the paper ballots are inspected by humans, can reliably detect any cyberattack that might have altered the election

[23] Volkswagen used a similar strategy to conceal the way it circumvented EPA emissions tests: http://www.reuters.com/article/us-volkswagen-emissions-audi-idUSKBN1370Q3

outcome on the optical scanners. A manual recount is the best way, and indeed the only way, to ensure public confidence that the results are accurate, authentic, and untainted by interference.

35. Manual recounts are not necessarily more time-consuming than recounting using optical scanners, particularly when only one race is being counted. A manual recount focuses on a single contest, and human observers typically proceed by sorting the ballots into stacks according to the chosen candidate and then counting the ballots in each stack. This is an efficient and straightforward process. If scanners are used, the scanners must be programmed and tested, new removable media must be located and programmed, and the ballots must be fed into the scanner by humans. These steps are not necessary when hand counting is used.

36. The paper ballots used in Pennsylvania can be counted much more easily and reliably than the punched card paper ballots that were recounted in Florida during the 2000 presidential election. Punched card ballots are fragile, so each time they are counted, the record of voters' intent may be inadvertently altered. They are also difficult to interpret, sometimes requiring a magnifying glass to discern whether the voter intended to make a mark. Pennsylvania's optically scanned paper ballots are a completely different technology. They create a persistent and readily interpretable record of voters' intent that does not suffer from these problems, and they can be counted efficiently and accurately in a manual recount.

37. Examining the available physical evidence, including paper ballots, paper vote records, and the voting equipment itself, will set a precedent that will provide an important deterrent against cyberattacks on future elections. By performing a rigorous recount now in a method that would detect cyberattacks affecting the outcome (that is, by thoroughly examining this physical evidence), we send a strong signal to attackers that any future computer-based tampering efforts are likely to be caught.

This affidavit was executed on the 30th day of November, 2016 in Ann Arbor, Michigan.

J. ALEX HALDERMAN

Sworn to before me this 30th day of November, 2016.

Tobin C Darnell
Notary Public

My Commission Expires: 04-04-2018

TOBIN C. DARNELL
NOTARY PUBLIC, STATE OF MI
COUNTY OF WASHTENAW
MY COMMISSION EXPIRES Apr 4, 2018

AFFIDAVIT OF HARRI HURSTI

I declare under penalty of perjury under the laws of Pennsylvania that the following is true and correct.

1. I submit this Affidavit in support of petitions to recount/recanvass the vote in Montgomery County, Pennsylvania.

2. I have been a consultant and a co-author of several studies commissioned or funded by various U.S. states and the federal government on computer security. In the area of election security, I am the co-author of several peer-reviewed and state-sponsored studies of election system vulnerabilities. Most notably, I was a co-author of the EVEREST comissioned by the Secretary of State of Ohio (http://hursti.net/docs/everest.pdf), a study of vulnerabilities in Sequoia AVC voting machines (http://hursti.net/docs/princeton-sequoia.pdf), and a study of the Estonian Internet voting system (http://hursti.net/docs/ivoting-ccs14.pdf). In 2005, I developed the Hursti Hack(s), a series of four tests in which I demonstrated how voting results produced by Diebold Election Systems voting machines could be altered. I have served as an expert on electronic voting issues in consultations to officials, legislators, and policy makers in five countries. I received the Electronic Frontier Foundation's EFFI Winston Smith Award in 2008, and the Electronic Frontier Foundation EFF Pioneer Award in 2009 for my research and work on election security, data security and data privacy. I recently founded Nordic Innovation Labs to advise governments around the world on election vulnerabilities. My qualifications and experience are further detailed at the following website: https://nordicinnovationlabs.com/team/harri-hursti/.

How AVC Advantage Machines Work

3. According to VerifiedVoting.org,[1] Montgomery County uses direct recording electronic ("DRE") voting machines called Sequoia AVC Advantage. I have studied these machines in detail, including for a report submitted to the New Jersey Supreme Court.

4. With respect to all DRE machines, including the AVC Advantage, the voter indicates a selection of candidates via a user-interface to a computer; the program in the computer stores data in its memory that (are supposed to) correspond to the indicated votes; and at the close of the polls, the computer outputs (what are supposed to be) the number of votes for each candidate.

5. For the AVC Advantage, electronic ballot definitions are prepared and results are tallied with a Windows application called "WinEDS" that runs on computers at election headquarters in each county. Ballot definitions (contests, candidate names, party affiliations, etc.) are transmitted to the Advantage via a "results cartridge," which is inserted at the election warehouse before the machines are transported to polling places before the election. The votes cast on an individual machine are recorded in the same cartridge, which poll-workers bring to election headquarters after polls close.

6. The AVC Advantage 9.00 includes an "audio kit" containing its own computer board. Any voter who wishes to vote by audio instead of on the large printed buttons-and-lights voter panel is permitted to do so. Voters might wish to vote by audio because of vision impairments, mobility impairments, inability to read, or for any other reason; indeed, voters are not required to state the reason they wish to vote by audio.

[1] https://www.verifiedvoting.org/verifier/#year/2016/state/42/county/91.

7. The audio-kit computer resides on a "daughterboard" inside the cabinet but separate from the main circuit board of the AVC Advantage (which is called the "motherboard").

8. Unlike the motherboard firmware, the firmware of the daughterboard does not reside in read-only memory ("ROM"). It resides in "flash memory"; the flash memory contains the election control program, as well as ballot definitions and other files. Unlike ROM, which cannot be modified without removing and replacing physical computer chips, flash memory can be written and rewritten by the software (or firmware) inside the computer.

AVC Advantage Machines Are Vulnerable and Not Reliable

9. Our study of the AVC Advantage machines found that the AVC Advantage is vulnerable to election fraud, via firmware replacement and other means. Even in the absence of fraud, the AVC Advantage has user interface flaws that could cause votes not to be counted.

10. As we explained in our report, the AVC Advantage is easily "hacked" by tampering with the machine's firmware. Because there is no paper receipt, all electronic records of the votes are under control of the firmware, which can manipulate them all simultaneously.

11. Without even touching a single AVC Advantage, an attacker can install fraudulent firmware into many AVC Advantage machines by viral propagation through audio-ballot cartridges. The virus can steal the votes of blind voters, can cause AVC Advantages in targeted precincts to fail to operate; or can cause WinEDS software to tally votes inaccurately.

12. AVC Advantage Results Cartridges can be easily manipulated to change votes, after the polls are closed but before results from different precincts are cumulated together.

13. The vulnerability of the machines means that good-faith programming errors can also manipulate votes, even without malicious intent. The outdated software renders the machines prone to errors that could affect vote totals.

14. There are also major user interface flaws that may cause inaccuracy in counting votes, including that the AVC Advantage sometimes appears to record a vote when in fact it does not, and vice versa.

These DRE Machines Are Susceptible to Fraud and Tampering

15. The AVC Advantage machines are vulnerable to fraud and inadvertent tampering in a variety of ways. Specifically, the daughterboard and the WinEDS system renders them particularly vulnerable to tampering, fraud, and virus infection.

16. For example, as described above, in addition to the Z80 computer on the AVC Advantage motherboard, the AVC Advantage version 9.00 contains a second computer, called the daughterboard, which is used in audio voting.

17. One can install fraudulent firmware into the daughterboard simply by inserting an audio-ballot cartridge infected with a virus into the slot in the daughterboard. An honest elections official who is unaware of the presence of the virus can do this unwittingly. The process takes one or two minutes. One virus can propagate onto all the WinEDS computers and AVC Advantage voting machines used in a county. This is a very severe vulnerability.

18. Fraudulent firmware in the daughterboard can steal the votes of blind voters, or of any voters who use audio voting, and can selectively cause voting machines to fail on election day in precincts chosen by the attacker.

19. On the version 9 AVC Advantage, the daughterboard does not directly write votes to the Results Cartridge. The motherboard controls the Results Cartridge, and communicates with the daughterboard via messages sent through a cable. When a voter votes using audio, the daughterboard presents the ballot aurally to the voter, and communicates candidate selections to the motherboard.

20. Audio voters use an input device that is connected to the daughterboard, not the motherboard. Thus it is very easy for fraudulent daughterboard firmware to steal the votes of audio voters, simply by conveying different candidate choices to the motherboard. The votes of disabled voters are even more at risk, on the AVC Advantage, than the votes of those who use the full-face voter panel.

21. In addition, the attacker can cause voting machines to fail in a selected set of precincts. For example, if he disables a dozen or two voting machines in heavily populated districts across the state, then long lines of voters may form, and some voters may leave the polling place before voting. The significance of doing this attack via a daughterboard virus is that a single person can disable voting machines in hundreds of precincts that he chooses, without ever going near any of those machines.

22. To do this, the attacker then programs an audio-ballot virus, replacing the audio-voting software on the daughterboards of all AVC Advantage voting machines in the county.

23. On election day, when each machine is turned on, one of the first things that the motherboard does is to send a message to the daughterboard saying (paraphrase) "load the audio ballot," and the daughterboard normally responds saying (paraphrase) "OK." However, the

fraudulent daughterboard software responds with a different message, either one of the following:

- "Cannot load ballot." Then the AVC Advantage (motherboard) will display an error message on the Operator Panel, and the election cannot start.
- A specially crafted message that triggers a buffer overrun bug. This causes the machine to reboot, in an infinite loop, or for as many repetitions as the daughterboard chooses.

In either case, the AVC Advantage will fail to start up on the morning of election day, or will be delayed for a chosen number of minutes.

24. The audio-ballot cartridge loaded in the daughterboard contains the name and number of the election district in which the machine will be used. Thus the daughterboard firmware has enough information for an attack on specific precincts. This allows a selective denial of service to specific demographic groups.

25. This general means of manipulating elections is well understood. In Ohio in the 2004 Presidential election, it was widely reported in the press that the misallocation of voting machines led to unprecedented long lines that disenfranchised scores, if not hundreds of thousands, of voters. Selective disabling, instead of misallocation, could produce a similar result.

26. The daughterboard virus is a very elementary attack. Virus programming is not much taught in schools, but unfortunately there are many practitioners of it nonetheless. The number of known computer viruses is enormous. The virus definition file maintained by the virus detection firm Symantec lists over 17 million separate virus "signatures."

27. For this particular virus programming, not even a bachelor's-degree level of skill is necessary. The daughterboard is an Intel-486-compatible computer running a DOS operating

system—just like the hardware and software of the IBM PCs from about 1990. Millions of PC users gained familiarity with its scripting tools that would be helpful in creating viruses for the AVC Advantage daughterboard.

28. We found that it is also possible to reverse-engineer the daughterboard firmware. The daughterboard computer is made by Compulab. We were able to find documentation for this computer on the Internet. Compulab sold this computer for many applications, not just voting machines, and development tools are available for it. Using these development tools, an attacker could extract the firmware and reverse-engineer it. Then, using the results of this analysis, he could devise fraudulent firmware of the kind we described above.

29. The motherboard is also vulnerable to malicious daughterboard firmware. One might hope that disabling audio voting would make the motherboard immune to harmful effects from a daughterboard virus. Unfortunately, this is not the case. Because of a mistake Sequoia made in programming the motherboard firmware, the AVC Advantage is vulnerable even if the ballot definition says not to use audio voting.

30. In addition to the daughterboard, the WinEDS system is vulnerable to fraud and tampering. Election workers prepare ballots for the AVC Advantage on WinEDS computers at the election warehouse, or at the board of elections, or other locations. The electronic ballot definition loaded into the Results Cartridge specifies not only the names of the candidates, but several other options about the election. In preparing a ballot definition for the AVC Advantage, one can choose the option to disable audio voting. The (large-format) Results Cartridge with this option setting is then loaded into the (motherboard of the) of the AVC Advantage. This tells the motherboard not to use the daughterboard.

31. The WinEDS election-management software is known to be insecure, based on studies done by the State of California. In our examination we noticed some of the same weaknesses in WinEDS that were previously reported elsewhere.

32. In summary, AVC Advantage voting machines and WinEDS vote-tabulation software are both severely vulnerable to viruses that can alter election results. We have demonstrated the feasibility of creating a computer virus that propagates from AVC Advantage machines to each other, and to WinEDS computers. Such a virus can carry payloads that modify votes inside the AVC Advantage, and modify election and vote databases in WinEDS. The virus can also be programmed to erase itself from voting machines just before the polls close, so as to avoid detection after the fact.

Without A Forensic Evaluation It Is Impossible To Whether the Original Tally Can Be Trusted

33. Because of these numerous vulnerabilities, a full forensic evaluation by independent experts of all of the component's of Montgomery County's Sequoia voting system used in the 2016 presidential general election is the minimum requirement to have any trust at all that the vote was accurately recorded and tallied. This includes:

a. Every computer on which Sequoia's WinEDS software was used during the election cycle to prepare Montgomery County's electronic ballot definitions and audio ballots and tabulate results;

b. A randomly selected sampling of Sequoia AVC Advantage electronic voting machines, with audio-ballot kits installed and on which ballots were cast. At a minimum, a randomly selected sample of audio-ballot cartridges and results cartridges; and

c. The audio ballot cartridge and results cartridge used for those Sequoia Advantage machines.

34. Without such a forensic evaluation, there can be no confidence in the election results.

35. Simply instructing the WinEDS computer to display or print out the results will accomplish nothing. The result will necessarily be identical to the initial computation. This achieves nothing by way of verifying the accuracy or integrity of the results.

36. Similarly, re-uploading the results stored on the results cartridges from the Sequoia AVC Advantage machines used in the election to the WinEDS computer would be an empty exercise. Absent intervening tampering, the results stored electronically on each cartridge will be the same as they were at the time of the initial upload.

37. By contrast, forensic examination by independent experts of the audio-ballot cartridges inside one or more of the AVC Advantage machines used in the election could produce evidence that the software resident on the cartridges had been infected with a virus capable of switching votes from one candidate to another or rendering the affected AVC Advantage machine inoperable on Election Day. It may then be possible to demonstrate the precise nature of any vote-switching routine and its corrupting effect on the recording of votes for a candidate other than the one intended by the voter.

40. Forensic examination of the WinEDS computer used by the county could produce evidence that the WinEDS election management software installed on the computer had been

tampered with. Such tampering could be accomplished through direct physical access to the computer, connection of the computer to the Internet at any time before the election, or infection by a virus on one of the audio ballot cartridges that had been connected to the WinEDS computer for programming.

Executed on the 30th day of November, 2016 in Helsinki, Finland.

HARRI HURSTI

AFFIDAVIT OF DANIEL LOPRESTI

I declare under penalty of perjury under the laws of Pennsylvania that the following is true and correct.

1. I am the Chair of the Department of Computer Science and Engineering at Lehigh University. I was a founding research staff member at the Matsushita Information Technology Laboratory in Princeton, and later served on the research staff at Bell Labs working on document analysis, handwriting recognition, and biometric security. At Lehigh, my research examines fundamental algorithmic and systems-related questions in pattern recognition, bioinformatics, and computer security.

2. I submit this affidavit in support of petitions to recount/recanvass the vote in Philadelphia County and Montgomery County.

3. I believe that the direct recording electronic ("DRE") voting machines used throughout Pennsylvania, including Philadelphia and Montgomery counties, are vulnerable to fraud, tampering, and hacking, and are unreliable.

The Machines Used in Philadelphia and Montgomery Counties Are Vulnerable

4. In early 2007, I acquired a Danaher Shouptronic ("Shouptronic") 1242 full-face DRE voting machine, the type of electronic voting machine used in Philadelphia County.[1] I examined the machine and supervised its dismantling by a Lehigh student to understand how the machine functions and to identify its vulnerabilities. This included identifying the ROM chip which stores the machine's firmware (i.e., built-in programming) and the microprocessor that controls the operation of the machine. I also reviewed the

[1] *See* https://www.verifiedvoting.org/verifier/#year/2016/state/42/county/101.

manufacturer's manual entitled "Shouptronic 1242 Election System Information and Technical Specifications." (Shouptronic is now known as Danaher.)

5. At the same time, I also acquired a Sequoia AVC Advantage full-face DRE, the type of voting machine used in Montgomery County. Along with another Lehigh student, I opened the rear panel of the Advantage and examined its construction. This included identifying the ROM chips which store the machine's firmware (i.e., built-in programming) and the microprocessor that controls the operation of the machine. I also reviewed the manufacturer's manual on security entitled "AVC Advantage Security Overview."

6. In my opinion, none of the DREs certified in Pennsylvania, including the AVC Advantage and the Shouptronic 1242, is capable of retaining a permanent physical record of each vote cast as required by the Pennsylvania Election Code. As such, the machines cannot be said to reflect the actual tally of votes with 100% certainty.

7. My opinions are based on by own independent review and knowledge of the types of machines in question, as well as well-documented results of later examinations conducted by independent technical experts in other states that have identified serious security vulnerabilities in DRE systems that had previously been certified for use in Pennsylvania. Voting systems deemed acceptable for use in Pennsylvania were later found to be unacceptable for use in California and Ohio based on evaluations using testing methodologies widely known and practiced in the field of software security.

How DRE Machines Work

8. Each DRE voting system is designed to, and ostensibly does, record the voter's choices on various forms of computer memory. Electronic memory technologies used in DRE systems include:

   a. RAM (random access memory): electronic memory that is freely readable and writable under software control, but whose contents are not maintained when electrical power is turned off to the system. RAM can be further subdivided into "dynamic" RAM, or DRAM, and "static" RAM, or SRAM, a distinction which is important at the hardware level but not with respect to how information is stored. Because RAM is volatile memory, it is most often used for the temporary storage of data and program code in voting systems, and not for information which must be maintained after the machine is turned off. RAM is the most common form of memory in a computer system, so generic references to "computer memory" or "internal memory" usually refer to RAM. DRE systems sometimes provide a small amount of SRAM with a battery backup so that its contents can be maintained over time.

   b. PROM (programmable read-only memory): memory which is permanently programmed at the time of manufacture and hence is unalterable. As a result, PROM is used in "read-only" mode. PROM cannot be used to store vote data, rather, it is used in DRE systems to hold the machine's program code (firmware). PROM is often socketed to make it easier for the manufacturer of the system to install firmware updates by swapping a newer PROM chip for an older one without risking damage to the circuit board.

c. EPROM (erasable programmable read-only memory): non-volatile memory that can be programmed using a device that supplies higher voltages than a standard electronic circuit used for other memory technologies. Because EPROM is non-volatile, it retains its data even after electric power has been turned off. The contents of an EPROM are erased by exposing the chip to strong ultraviolet light; an EPROM must be erased before data can be written to it. EPROM can be used to hold firmware and/or vote data. Exposure to normal light may make EPROM storage unreliable as most forms of light (including daylight) contain some amount of ultraviolet light. EPROMS are often found socketed for ease of replacement.

d. EEPROM (electrically erasable programmable read-only memory): non-volatile memory that can be read and written in a standard electronic circuit. In this way EEPROM is similar to RAM, although it retains its data when power is turned off and is more expensive than RAM.

e. Flash memory: a form of EEPROM that differs from traditional EEPROM in the way the memory is written: byte-wise writable memories are typically referred to as EEPROM, whereas block-wise writable memories are referred to as Flash memory.

f. PCMCIA ("Personal Computer Memory Card International Association"): frequently referenced in the voting machine literature, PCMCIA is not a memory technology, but rather a form factor and interface specification originally developed for memory expansion in laptop computers. A PCMCIA card may contain RAM or flash memory and is typically the size of a credit card. Some PCMCIA memory devices may have a "write-protect" option, but this has no effect until the feature is activated, usually through manually moving a physical switch to a pre-specified position.

9. The Shouptronic 1242 records voter choices in six different computer memory locations. Each machine uses a memory cartridge which is inserted in the back of the machine. The memory cartridge contains the ballot definition files which allows the machine to conduct elections. The cartridge also contains three distinct memories for storing vote data: one EPROM and two EEPROMs. Vote data is also stored inside the Shouptronic 1242 itself in three separate RAM locations.

10. The AVC Advantage full-face push button DRE voting system loads ballot definitions and stores vote data using a "Results Cartridge" PCMCIA card. The Advantage system also contains internal memory upon which vote data is stored.

The DRE Machines Are Unreliable and Susceptible to Tampering and Fraud

11. None of the computer memory technologies identified in the preceding paragraphs provide a permanent physical record of each vote cast. Rather, these systems maintain what is best described as an "electronic record" of the activity that occurs on the machine. The accuracy or permanence of data stored electronically cannot be guaranteed due to the inherent characteristics of electronic computer memory. All of the forms of computer memory used in the DRE voting systems cited earlier are freely writable under software control for the period of time that an election is taking place. Computer memory can be written or rewritten with incorrect data unintentionally (as a result of software and/or hardware and/or human error) or intentionally (as a result of a malicious attempt to alter the results of an election).

12. Moreover, the act of writing computer memory is in principle undetectable; it leaves behind no physical evidence. This is true even for flash memory modules that contain a manually activated switch or fuse to disable their rewritability at the end of the election; until writability is disabled, typically at the end of the election, the contents of the flash memory may be altered in arbitrary ways. Since even the initial writing of a record into computer memory is accomplished through the use of software and hardware intermediaries, there is no way for a human observer to confirm that what is written is in fact an accurate record of his/her vote. Software-based techniques that attempt to assure the integrity of the electronic record through, for example, cryptography or digital signatures are only as trustworthy as all of the software components that interact with the computer memory during the recording and tallying of votes.

13. Both the firmware used to direct the operation of DRE voting systems and the voting records stored in computer memory within those systems are vulnerable to tampering in a number of ways. This is true even when voting systems are not connected to the Internet. For example, the PROM chips containing a DRE's firmware can be swapped in a matter of minutes by someone with minimal technical knowledge who has access to the voting machine and a simple screwdriver. Computer security experts have demonstrated how voting machine viruses can be spread in some cases through the use of contaminated memory cards, even for DRE systems that have never been connected to the Internet. Undetected flaws in the programming of a DRE system can result in errors in the electronic voting record as it is stored or retrieved from the memory within the machine. Such undetected flaws can also create opportunities for "hackers" to manipulate the voting data stored in the memory of the DRE under certain circumstances.

A Forensic Analysis Is Necessary to Fully Recanvass/Recount the Vote

14. In my opinion, review of the ballot images retrieved from computer memory is not a reliable way to recanvass and/or recount the vote. A full forensic evaluation of the DRE machines and associated supporting hardware and software (e.g., the computers and software used to program the ballot definition files) is necessary to ascertain whether the original totals reported by the DRE machines represent the votes that were cast on those machines.

15. In the above DRE systems certified for use in Pennsylvania, ballot images are stored in the same forms of computer memory as all other election data, under control of the same hardware / software components. The printed ballots are no more than a convenient, human-intelligible reproduction of the electronic record. Because of the unavoidable and fundamental dependence on software and hardware intermediaries to recover ballot images stored in computer memory, because these same software and hardware intermediaries are also responsible for maintaining and producing the original totals tapes for the election, and because all election data, including the ballot images, are generally stored in equivalent forms of electronic computer memory, simply reviewing the images would not be a reliable way to recanvass or recount the vote.

16. A full forensic evaluation of the DRE systems and associated supporting hardware and software would allow examiners to determine whether or not the information stored in the computer memory in those systems represents an accurate record of the votes that were cast on those machines.

17. Based on my knowledge of the DRE systems in place in both Montgomery County and Philadelphia County, I believe that only a full forensic evaluation, by

independent experts, of the relevant materials (detailed below) can ensure that the votes in both counties were fully and accurately counted.

a. For the AVC Advantage machines, an independent expert must be able to forensically analyze (i) a sampling of the AVC Advantage machines including source code of the software running on those machines, (ii) the audio ballot cartridges, (iii) the results cartridges, and (iv) any computers and associated software used by Montgomery County for preparation of the AVC Advantage machines, including programming ballot definition files before the election and tallying results after the election.

b. For the Shouptronic machines, an independent expert must be able to forensically analyze: (i) a sampling of the Shouptronic 1242 machines including source code of the software running on those machines, (ii) the results cartridges, and (iii) any computers and associated software used by Philadelphia County for preparation of the Shouptronic 1242 machines, including programming ballot definition files before the election and tallying results after the election

Executed on the 29 day of November, 2016 in Northampton County, Pennsylvania.

DANIEL LOPRESTI

AFFIDAVIT OF S. CANDICE HOKE

I, S. Candice Hoke, duly sworn, depose and say the following under penalty of perjury:

1. My name is S. Candice Hoke. I am the Co-Director of the Center for Cybersecurity & Privacy Protection and a Professor of Law at Cleveland State University, Cleveland, Ohio. I reside in Pittsburgh, PA and am a registered to vote in Pennsylvania.

2. I hold a Master's of Science in Information Security Policy and Management from Carnegie Mellon University and a J.D. from Yale Law School. I have worked as a Cybersecurity Engineer as a member of the Cyber Risk & Resilience Team in the CERT Division of the Software Engineering Institute of Carnegie Mellon University.

3. My research focuses on election cybersecurity, cyber risk assessment, and data privacy. My published work and teaching include attention to the regulatory systems that govern electronic voting. I have also authored published works on election forensics, including a guide for election officials and their lawyers that the American Bar Association distributed in 2008 free of charge to all members of the Section on State and Local Government Law

4. I founded and directed the Center for Election Integrity, located at Cleveland State University, which focused on improving election administration throughout the nation and specifically on the discovery and effective management of security vulnerabilities present in deployed voting equipment.

5. When Cuyahoga County, one of the largest election jurisdictions in the nation, first launched its e-voting system and suffered a major election disaster in which every technical and management system failed (May 2006), the Cuyahoga County Board of Elections and the County Commission jointly appointed me to a 3-person investigatory panel to ascertain the causes and cures. In that capacity, I worked to secure a forensics review of the absentee ballot scanners that intermittently had miscounted ballots, and hired and supervised investigatory

staff, leading the technical team in its overall assessment of operational and software election security. I was the major author of the Final Report that included over 300 action recommendations for improving the election process and its electronic voting systems.

6. After the Cuyahoga Election Review Panel submitted its report and recommendations, including the forensics evaluation, the same public bodies then appointed the Center for Election Integrity (of which I was the Director) to serve as Public Monitor of Cuyahoga Election Reform. I then worked for the next two years in that role, and was closely involved with the ongoing assessment and improvement of voting system security in Cuyahoga County (2006-08). I observed and documented in written reports various security vulnerabilities in actual elections operations, and violations of security policies. I was also involved in voting system procurement decisions when the County decided to replace its DRE precinct systems and move to optical scan systems with post-election auditing after every election.

7. While I was living in Ohio, I also served within the election system as a supervising poll worker; as a "roving" election technology trouble-shooter for many voting locations; as a voter registration problem-solver; and as a consultant to the Ohio Secretary of State's office on election management and improvement, including on voting technology issues.

8. In my academic capacity I have published peer-reviewed research that analyzes the security of electronic voting systems currently deployed in Pennsylvania, Ohio, California, and many other States. I was part of a team of experts commissioned by the California Secretary of State to conduct a "Top-to-Bottom Review" of that state's voting systems, specifically serving as a Research Team Leader for a portion of the Diebold study. I also served as a pro bono consultant to the Ohio Secretary of State in structuring that voting system security study.

The DRE Machines Used in Pennsylvania Are Vulnerable

9. All of the direct recording electronic (DREs) voting machines that Pennsylvania deployed in 2016 were designed to use software components that have been out of date for more than a decade. As such, they are pervaded with well-documented operational reliability and security deficiencies that can be easily yet covertly exploited in ways that can cause great harm to important data and systems.

10. All DRE voting systems offer the opportunity for covert tampering with memory media in ways that can lead to the central tabulator software or the election management system (EMS) to be infected with a virus or other malware that can lead to false vote counts. Because many counties outsource election services to vendors -- including for creating the electronic ballots and configuring the EMS database for tallying votes and for programming, testing, or delivering the DRE units to polling location—a wealth of opportunities exist for tampering with the election system to change the behavior of the software in ways that can cause them to deliberately miscount.

11. DRE systems currently deployed in Pennsylvania use antiquated and unreliable memory media to record votes. The vote aggregation methods among multiple DRE units at a precinct often confuse poll workers, and has not infrequently led to some memory cartridges not being tabulated or returned to the election office in a timely manner. Fortunately, some vendors of some of the voting systems used in Pennsylvania designed their systems to alert election officials when any of the DRE memory media are missing from the tabulations, so that the officials can seek out the location of that missing media and record the votes. But other DRE systems deployed in the Commonwealth lack that essential feature and thus render it exceptionally easy to miss some votes and produce inaccurate vote tallies.

12. The antiquated DRE touchscreens have been deployed well past their recommended life cycle, and not surprisingly, are losing their ability to respond accurately to voters'

selections. This problem can result in "vote flipping" between candidates. DRE touchscreens can also be misprogrammed - deliberately or accidentally—in ways that can cause the votes not to track accurately. Logic and Accuracy (L & A testing) in advance of elections is supposed to catch and provide the opportunity to correct such errors before voters cast their ballots. But few election jurisdictions use the depth and scope of L & A testing required to assure that their DRE systems have not been misprogrammed or have "rogue code" planted on them. Malware and code designed to mis-record voters' choices by changing votes to count for other candidates can be designed to activate only at a certain time after the L & A testing, and there are many other ways for cheating code to avoid being detected by L&A tests.

13. The DREs cannot function without an EMS configuring the ballot and generating the "instructions" that the DRE will use for presenting the ballot to the voter and recording the cast votes. Hence, the EMS and DRE vulnerabilities - both as to security and reliability -- are interrelated and impact one another.

14. As examples of how normal functioning of a poorly designed EMS can lead to the vote tabulation database "dumping" data - i.e., votes -- or "corrupting" that data, I would submit the experience of Cuyahoga County, Ohio. Because I served as the Project Director of the Public Monitor of Cuyahoga Election Reform, and had convened a technical team with access to tabulation records, we were able to publicly document that in the May 2006 primary, the GEMS database grew beyond the capacity that software could handle. Concretely, this meant that as DRE vote media and the scanned absentee ballot batches were uploaded to the GEMS server, GEMS covertly - without notice to officials-- dumped some of that data because its Microsoft JET / Access database foundation was not able to manage that amount of data. As a result, hundreds of votes in one county alone were not recorded and recounts determined that some previously announced winners actually had not won.

15. In the November general election of 2006, while preparing for the election and then on election night during the tabulations, the GEMS servers were repeatedly crashing. As Monitor, we staffed the tabulation server room and noted each time the server crashed; the security plan also required that an official record be made of each and every server crash, with its time and operator input when it occurred. Because we knew that servers crashing during tabulations could cause data corruption, we sought a forensic review of the database to ascertain whether vote data integrity had been preserved. We documented a number of indicators of data corruption, including database table element entries that missed their date/time stamps of when the information was entered; other tabulation entries' date/time stamps were marked "January 1, 1970," which is the epoch (zero- point) of UNIX time—rather than carrying the 2006 date and time. Finally, vote totals in two separate database tables held different values for the candidates' results, differing by hundreds of votes.

A Fornsic Evaluation of the DREs Is the Only Way to Determine the Accuracy of the Vote

16. Given (a) the multiple available pathways for inserting malware or code that can cause vote flipping or miscounts; (b) the clear existence and motivation of numerous skilled and motivated hackers, including from nation-state adversaries; (c) the unreliability of the systems owing to their age and defective software designs, and (d) repeated crashing during pre-election and election tabulations, a recount that includes a forensics assessment of the EMS and at least a random selection of the DREs and associated components is necessary to ascertain whether the reported tallies are accurate.

17. Voting system experts who have no financial relationship to the vendors or their contracts, and who have developed expertise in these systems deployed in the Commonwealth can efficiently conduct forensics reviews in a targeted manner, focusing on the main frailties in these systems. For instance, in one 2-hour session in Cuyahoga County, one Monitor staff database examiner was able to document all the irregularities mentioned in paragraph 15,

supra. While most forensics assessments would not proceed this quickly, and investigating and correcting for the anomalies consumed some additional time, valuable information can be obtained in a matter of hours regarding whether the system performed as expected and required. . Forensics reviews are the only means to check whether all these functions are performed accurately for all-electronic DRE systems.

18. One of the additional values of an independent forensics review is that it allows the public and public authorities to obtain essential information relevant to whether and when they choose to replace the dilapidated voting systems. In Cuyahoga County, for instance, the officials made a decision to replace the GEMS-and-DRE system because it proved to be too unreliable and difficult to manage in a secure manner. In barely 1.5 years after our reports documenting these operational and the software architectural issues (that the vendor had hidden and that could not be fixed without a wholesale re-architecting of the software), Cuyahoga County chose to replace its voting system with a more reliable and accurate option.

19. Although I have personally listened to fears of election and other public officials that they will be accused of wrongdoing, or that the public will blame them personally for any problems that are discovered in a forensics review of election systems, or that the voting public will refuse to participate in voting if they learn of technical and other deficiencies in their election equipment, I would like to relate what occurred in Cuyahoga County. The May 2006 Federal primary election vote tally reports proved to be unreliable and inaccurate, in at least some races, and serious public questions were raised about the adequacy of the voting technologies. Instead of a superficial fix, our County's appointed independent investigatory team endeavored to figure out everything that had gone wrong, technically and managerially, and to disclose everything in public reports. We sought to assure the public that their voting rights were protected and that their choices would be accurately recorded and tabulated at least in future elections. We asked for the public's participation via public hearings on their

experiences and concerns, and retooled poll worker recruitment and training to ensure that fewer errors could occur at the polls. The public responded vigorously, attending standing room only public hearings and producing a large number of new volunteers to work as poll worker and in other roles. That fall, for the general election, our voting participation rates rose instead of falling and we had scores of new citizens involved in the election system in a variety of roles, all proving that transparency on voting problems can produce public energy and dedication to participate as well as help improve the election system.

20. As a voting systems and election administration specialist, and as cyber risk expert, I am concerned that hackers and other miscreants have learned that Pennsylvania has erected a series of legal obstacles that generally inhibit checking into the integrity of county election tabulations. Thinking from the security perspective, this legal cover basically provides a neon sign to motivated hackers both domestically and abroad, saying "*Come Hack Here; we won't be checking.*" Hackers seek valuable and preferably unprotected targets, and those who have been documented by Federal authorities to have interfered in this election cycle would have been highly motivated to try to probe and impact Pennsylvania's systems. As an election management and security specialist, I recommend that Pennsylvania clearly establish that its elections are not open to any motivated hacker and that the Commonwealth assures that accurate voting tallies are generated without incursion by unauthorized others.

This affidavit was executed on the 2nd day of December, 2016, in Cleveland, Ohio.

S Candice Hoke

S. Candice Hoke

Sworn before me this 2nd day of December, 2016.

K. J. Kow

Notary Public

My Commission expires: KENNETH J. KOWALSKI, Atty.
NOTARY PUBLIC • STATE OF OHIO
My commission has no expiration date
Section 147.03 O.R.C.

AFFIDAVIT OF MATTHEW A. BISHOP

I, Matthew A. Bishop, duly sworn, depose and say the following under penalty of perjury:

1. My name is Matthew Bishop. I am a co-director of the Computer Security Laboratory and a Professor of Computer Science at the University of California at Davis.

2. I received a Master of Arts degree in Mathematics from the University of California at Berkeley and a Master of Science and Ph.D. in Computer Science, both from Purdue University. I have worked as a systems programmer at Megatest Corp., a research scientist at the Research Institute for Advanced Computer Science, and as a faculty member in the Department of Mathematics and Computer Science at Dartmouth College and in the Department of Computer Science at the University of California at Davis, where I am now a full professor.

3. As a computer security researcher, I have devoted a major portion of my research on the security and accuracy of electronic voting systems, as well as modeling the procedures and processes with which an election is conducted. Here, my use of the term "voting systems" includes the central software system that is used to create the ballots and that aggregates and records the votes in a database before reporting the election tallies (often called the "EMS" or election management system); the direct recording electronic (DRE) voting devices that present electronic ballots to voters for their choices to be recorded; the DRE memory media that records the votes; the optical scanners used at some polls to read voter-marked paper ballots; the optical scanners used at a central location (for tabulating absentee ballots and for re-tabulating in the

official canvass the polling locations' op scan ballots); and any other module or component that is attached to or integrates with the EMS or voting devices to conduct the election.

4. I have been an active researcher in voting system security, examining software and hardware, operational usability, and election equipment forensics for over twelve years. In addition to scholarly research and numerous publications on voting systems security and forensics, and working directly with election officials who seek to improve their election security and other processes, my field experience with e-voting systems includes assessing the state of electronic voting systems before purchase (California), penetration testing of Diebold TS DRE systems (Maryland), a post-election forensics evaluation in a contested election (Florida, on the ES&S iVotronic, a model I understand to have been used in Allegheny County precincts in 2016), and co-leading a comprehensive study of the security and accuracy of voting system certified for use in California, undertaken for the California Secretary of State in the "Top to Bottom Review."

5. The California Secretary of State's charge to the Top-to-Bottom Review technical team asked whether "the systems currently certified should be left alone, or specific procedures required to provide additional protections for their use, or the machines simply decertified and banned from use" (Overview of Red Team Reports, §2.0, p. 1). I led the the "red team" penetration tests, and had access to the work of the other teams, including the source code reviews. The summary Red Team Report given to the Secretary concluded that "the security mechanisms [manufacturers had] provided for all systems analyzed ***were inadequate to ensure accuracy and integrity of the election results*** and of the systems that provide those results" (Overview of Red Team Reports, §6.4, p. 11; emphasis added). The systems analyzed included the Diebold GEMS 1.18.24/AccuVote, The Diebold Accuvote-TSX with AccuView Printer Module and Ballot Station Firmware version 4.6.4, the Hart Intercivic System 6.2.1 including the

eSlate/DAU version 4.2.13 and the eScan version 1.3.14, and the Sequoia WinEDS version 3.1.012/Edge/Insight/400-C.

6. From my review of information on the web about Pennsylvania's voting systems deployed in 2016, it appears that the California systems I studied in depth in the Top to Bottom Review, in the Maryland penetration tests, and in Florida's Congressional 13 race, all overlap significantly with those that Pennsylvania deployed in 2016.[1]

DREs Are Unreliable and Vulnerable to Interference

7. Voting system security experts, including myself, have documented many vulnerabilities that can offer myriad covert opportunities for a motivated attacker to tamper with Pennsylvania's voting systems and ultimately cause the election tallies to fail to reflect the voters' choices.

8. "Hacking" or attacking the system is not the only type of problem with voting systems that can lead to inaccurate results. The accuracy of the election data, and specifically the electoral results, can be marred—sometimes significantly—simply because the software was not designed with the application of appropriate safeguards, coding principles, or database designs. These are some of the many types of software problems that have been documented in peer-reviewed scientific studies as well as in reviews of voting systems by others and myself.

9. As an example of an issue that speaks to the accuracy and integrity of the (formerly Diebold) GEMS software that is used to aggregate votes from e-voting systems and scanners and then tabulation and report results, all versions of the GEMS software that I have examined rely on the Microsoft Access database, which is built on top of software called the "JET engine." For the latest version of Microsoft Access, Access 2016, the maximum table size

[1] See for example http://www.dos.pa.gov/VotingElections/OtherServicesEvents/Pages/Voting-Systems.aspx#.VIhhucIRqPI

is 2 GB of data; extending this requires using multiple database files linked together. A database can hold no more than 32,768 objects, which in the context of an election would be ballots or votes.[2] These limits also hold in earlier versions of Microsoft Access, for example Access 2007[3] and Access 2010.[4] It is unclear what will happen if these data limits are exceeded. In the world of software, this is called "undefined behavior" and in elections, this uncertainty could result in inaccurate tabulations. As an example, on some computers,[5] adding 65535 + 65535 produces 65534, not 131,070 because the behavior of adding the two numbers exceeds the maximum number that the computer can store.

10. The software in the voting systems that I have personally studied have numerous flaws, including the addition flaw above. Some of these flaws could lead to incorrect recording of votes, or incorrect vote totals. These outcomes could occur in the absence of attacks.

11. There is considerable basis for doubting whether these voting systems are accurate and robust enough to produce trustworthy, accurate electoral tallies in general elections. We found that the systems used in California were not, as of the summer of 2007, despite having been certified to meet the requisite e-voting standards. Without access to the source code and to the systems themselves, it is impossible to know whether these problems, or other problems related to the accuracy and integrity of the systems, exist.

A Post-election Forensic Evaluations Is Necessary

12. The goal of a forensic examination of e-voting systems is to determine whether problems occurred that affected the accuracy and integrity of the system(s) and data in question.

[2] See *Access 2016 Specifications* at https://support.office.com/en-us/article/Access-2016-specifications-0cf3c66f-9cf2-4e32-9568-98c1025bb47c

[3] See *Access 2007 Specifications* at https://support.office.com/en-US/article/Access-2007-specifications-2EEDF198-6B27-4DC5-AE07-3E1FBA6D6C96

[4] See *Access 2010 Specifications* at https://support.office.com/en-US/article/Access-2010-specifications-1E521481-7F9A-46F7-8ED9-EA9DFF1FA854

[5] Specifically, computers with 16 bit integers.

This type of examination leads either to an increased confidence in the accuracy of the result, or an understanding of where and how the system made an error. An election system forensics examination may also lead to information that can be used to correct the errors in a manner that will allow the system to produce results that accurately reflect the voters' ballot choices.

13. A post-election forensics examination requires collecting and analyzing several types of data:

a. Records of any indication of failures such as an error message on a screen, and as much information about what happened and at what stage in the process it happened;

b. Records of any data relevant to the e-voting system, such as how physical access to the system was controlled;

c. Vote totals, electronic ballots, and any voter-verified paper audit trails or paper ballots; and

d. Source code and build procedures and environments, so the analysts can examine the software and, if necessary, regenerate it.

14. The steps in a forensic examination or audit can vary, depending on circumstances and what data is available. Basically, the analysts correlate the data they have, looking for inconsistencies and anomalies. They also (possibly concurrently) analyze the source code to determine if there are programming errors or inconsistencies that might cause problems, and if found determine whether those problems either occurred (ideally) or could have occurred. They can then attempt to reproduce those problems on the actual voting systems used in the election.

15. As an example, one of the first things the team would look at is the components of the software, how they interact, what their limits are, and what happens if those limits are

exceeded. This would, for example, answer the questions posed above about what happens if the Microsoft Access database limits are exceeded and large numbers are added together.

16. Assuring appropriate technical qualifications for team members is critical to the success of the forensic examination. Members of the team will need to analyze complex software, and how different integral components interact, often on a very tight timetable. Thus, some members of the team must be experts in computer security and forensic analysis. Further, at least one team member should have experience in analyzing e-voting systems, because that experience is invaluable to the entire team's efficiency. Perhaps most critical is a team member who has expertise and experience in how elections in the jurisdiction are administered, and the procedures normally used.

17. With the results of a forensic examination, the election officials, and the public, will have more confidence in both the results and the systems used in the election. It will show the concern and care that election officials have about the accuracy of the results of an election that they run. Even if problems were to be found, the fact that the public authorities have not hidden them but have sought to investigate promptly and publicly will increase the trust and confidence of voters in the way an election is conducted and the results verified.

Conclusion

18. My findings and experience in analyzing e-voting systems demonstrates that there is a considerable question as to whether these systems are accurate and robust enough for use in general elections. We found that the ones used in California were not, as of the summer of 2007, despite being certified to meet the requisite e-voting standards. Only a close evaluation of the source code and the voting systems will reveal whether Pennsylvania's voting systems were compromised with these same or similar vulnerabilities.

19. I understand that questions have been raised about the accuracy of the results of the election. A forensic examination, in which the examiners could analyze the components of the system, the data gathered during the election, and the results would help answer these questions. A manual recount where paper ballots are used would also answer these questions in those jurisdictions. These procedures would establish a high level of confidence in the results of the election.

20. Given the questions raised about the election results, I believe that these measures are appropriate and fully warranted.

This affidavit was executed on the 2nd day of December, 2016, in Davis, California.

Matthew A Bishop

Matthew A. Bishop

~~Sworn before me this 2nd day of December, 2016.~~

Please See California Jurat below.
GC 12/02/16

~~Notary Public~~

~~My Commission expires: ______________~~

A notary public or other officer completing this certificate verifies only the identity of the individual who signed the document to which this certificate is attached, and not the truthfulness, accuracy, or validity of that document.

State of California
County of Yolo
Subscribed and sworn to (or affirmed) before me on this 2nd day
of December, 2016, by Matthew A. Bishop
N/A, proved to me on the basis
of satisfactory evidence to be the person~~(s)~~ who appeared before me.
Signature ______________ (Seal)

GARY CHRISTENSEN
Commission # 2057618
Notary Public - California
Yolo County
My Comm. Expires Mar 11, 2018